Availability Analysis of a Scalable Intrusion Tolerant Architecture with Two Detection Modes

Toshikazu Uemura[1], Tadashi Dohi[1], and Naoto Kaio[2]

[1] Department of Information Engineering, Graduate School of Engineering
Hiroshima University, 1–4–1 Kagamiyama, Higashi-Hiroshima, 739–8527 Japan
[2] Department of Economic Informatics, Faculty of Economic Sciences
Hiroshima Shudo University, 1–1–1 Ohzukahigashi, Asaminami-ku, Hiroshima, 739–3195, Japan
dohi@rel.hiroshima-u.ac.jp, kaio@shudo-u.ac.jp

Abstract. In this paper we consider a discrete-time availability model of an intrusion tolerant system with two detection modes; automatic detection mode and manual detection mode. The stochastic behavior of the system is formulated by a discrete-time semi-Markov process and analyzed through an embedded Markov chain (EMC) approach. We derive the optimal switching time from an automatic detection mode to a manual detection mode, which maximizes the steady-state system availability. Numerical examples are presented for illustrating the optimal switching of detection mode and its availability performance. availability, detection mode, EMC approach, Cloud computing environment.

Keywords: SITAR, availability, intrusion tolerance, discrete-time modeling, detection mode, EMC approach, cloud computing circumstance.

1 Introduction

Cloud Computing is one of computing technologies in which dynamically scalable and often virtualized resources are provided as a service over the Internet. Since users need not have knowledge of expertise and the technology infrastructure in the network that supports them, recently this low-cost computing paradigm is becoming popular as an expected Internet-based computing in the next generation. Since the cloud computing is highly vulnerable to the Internet epidemics, many attacking events compromise a huge number of host computers rapidly and cause DoS around the Internet. Such epidemics result in extensive widespread damage costing billions of dollars, and countering the propagating worms in time becomes an increasingly emergency issue on the Internet security. Although traditional security approaches which may be categorized into *intrusion detection approaches* establish proactive barriers like a firewall, unfortunately, the efficiency of a single barrier is not still enough to prevent attack from sophisticated new skills by malicious attackers. As the result, the number of network attack incidents is tremendously increasing day by day. In contrast to pursue the nearly impossibility of a perfect barrier unit, the concept of *intrusion tolerance* is becoming much popular in recent years. An intrusion tolerant system can avoid severe security failures caused by intrusion and/or attack and can provide the intended services to users in a timely manner even under attack. This is inspired from traditional techniques commonly used for

M.G. Jaatun, G. Zhao, and C. Rong (Eds.): CloudCom 2009, LNCS 5931, pp. 178–189, 2009.

tolerating accidental faults in hardware and/or software systems, and can provide the system dependability which is defined as a property of a computer-based system, such that reliance can justifiably be placed on the service it delivers [1]. So far, most efforts in security have been focused on specification, design and implementation issues. In fact, several implementation techniques of intrusion tolerance at the architecture level have been developed for real computer-based systems. For an excellent survey on this research topic, see Deswarte and Powell [2].

In other words, since these methods can be categorized by a design diversity technique in secure systems and need much cost for the development, the effect on implementation has to be evaluated carefully and quantitatively. To assess quantitatively security effects of computer-based systems, reliability/performance evaluation with stochastic modeling is quite effective. Littlewood *et al*. [4] applied fundamental techniques in reliability theory to assess the security of operational software systems and proposed some quantitative security measures. Jonsson and Olovsson [3] also developed a quantitative method to study attacker's behavior with the empirical data observed in experiments. Ortalo, Deswarte and Kaaniche [7] used both privilege graph and Markov chain to evaluate system vulnerability, and derived the mean effort to security failure. Uemura and Dohi [8] focused on the typical DoS attacks for a server system and formulated an optimal patch management problem via continuous-time semi-Markov models (CTSMM). Recently, the same authors [9] considered a secure design of an intrusion tolerant database system [12] with a control parameter to switch an automatic detection mode to a manual detection mode after receiving an attack, and described its stochastic behavior by a CTSMM. In this way considerable attentions have been paid to stochastic modeling in security evaluation of computer-based systems.

In this paper we consider an existing system architecture with intrusion tolerance, called SITAR (Scalable Intrusion Tolerant Architecture). SITAR was developed in MCNC Inc. and Duke University [11]. Madan *et al*. [5], [6] considered the security evaluation of SITAR and described its stochastic behavior by a CTSMM. More precisely, they investigated effects of the intrusion tolerant architecture under some attack patterns such as DoS attacks. In this paper we consider the similar but somewhat different models from Madan *et al.* [5], [6]. By introducing an additional control parameter [9], [12], called the switching time from an automatic detection mode to a manual detection mode, we consider a discrete-time semi-Markov model (DTSMM). The authors considered in their previous work [10] to control the patch release timing from a vulnerable state. In COTS (commercial-off-the-shelf) distributed servers like SITAR, on the other hand, the intrusion-detection function equipped for a proactive security management is not perfect and is often switched to a manual detection mode, in order to detect intrusions/vulnerable parts more speedy [9], [12]. Then the problem here is to find the optimal switching time which maximizes the steady-state system availability. We describe the stochastic behavior of the underlying SITAR with two detection modes and develop an availability model based on a DTSMM.

The paper is organized as follows: In Section 2 we explain SITAR and describe the stochastic behavior [5], [6]. Section 3 concerns the EMC approach and obtain the representation of an embedded DTMC in a DTSMM. We derive the steady-state probability in the DTSMM by using the mean sojourn time and the steady-state probability

in the embedded DTMC. In Sections 4 and 5, we formulate the maximization problems of steady-state system availability in continuous-time and discrete-time cases, respectively. Actually, we showed in a different context that the control scheme which included auto patch would be useful to guarantee several security attributes [12], but at the same time that the design of the optimal PPMT was quite effective to optimize some quantitative measures [9]. We derive analytically the optimal PPMTs maximizing the system availability. It is worth mentioning in these optimization phases that the treatment of DTSMM is rather complex. Numerical examples are presented in Section 6 for illustrating the optimal preventive patch management policies and performing sensitivity analysis of model parameters. It is illustrated that the preventive patch management policies can improve effectively the system availability in some cases, and that the implementation of both preventive maintenance and intrusion tolerance may lead to keeping the whole Internet availability/survivability. Finally the paper is concluded with some remarks in Section 7.

2 SITAR

The SITAR is a COTS distributed server with an intrusion tolerant function [11] and consists of five major components; proxy server, acceptance monitor, ballot monitor, adaptive reconfiguration module, and audit control module. Since the usual COTS server is vulnerable for an intrusion from outside, an additional intrusion tolerant structure is introduced in SITAR. Madan *et al.* [5], [6] described the stochastic behavior of SITAR by means of CTSMM and gave its embedded DTMC representation. Figure 1 depicts the configuration of SITAR behavior under consideration. Let G be the normal state in which the COTS server can protect itself from adversaries. However, if a vulnerable part is detected by them, a state transition occurs from G to the vulnerable state V.

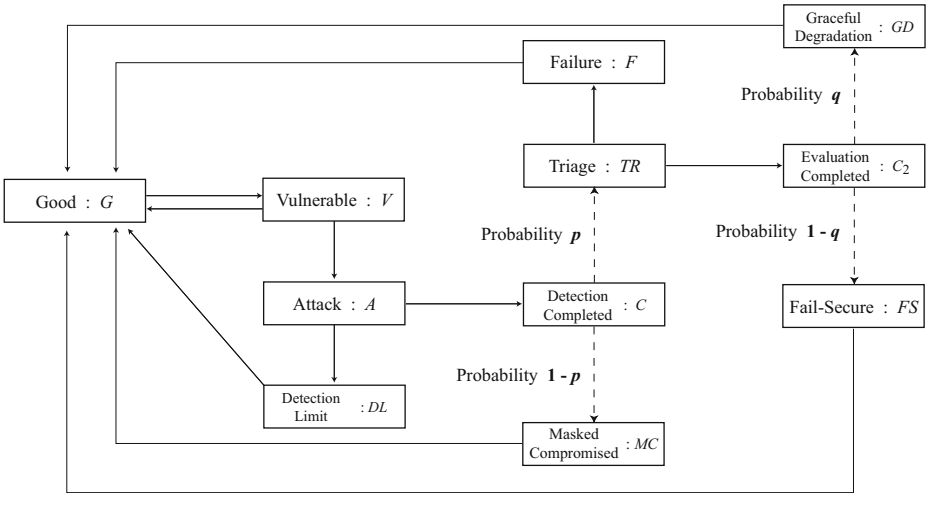

Fig. 1. Block diagram of SITAR behavior

Further if adversaries attack the vulnerable part, the state moves to A. On the other hand, if the vulnerable part is detected by vulnerability identifiers such as benign users, the vulnerable state V goes back to the normal state G again.

In the attack state A, two possible states can be taken. If the problem caused by the attack cannot be resolved and the containment of the damaged part fails, the corresponding event can be regarded as a security failure, and the initialization/reconfiguration of the system is performed as a corrective maintenance (repair) at DL. After completing it, the system state makes a transition to G again and becomes as good as new. While, if the intrusion/attack is detected, then the state goes to C. In the state C, one of two instantaneous transitions without time delay, which are denoted by dotted-lines in Fig. 1, can occur, *i.e.*, if the damaged part by attacking is not so significant and does not lead to a serious system failure directly, the system state makes a transition from C to MC with probability $1 - p$ $(0 \leq p \leq 1)$, and the damaged part can be contained by means of the fail safe function. After the containment, the system state moves back to G by masking the damaged part.

Otherwise, *i.e.* if the containment of the damaged part with serious effects to the system fails, the state goes to TR with probability p. We call this probability the *triage probability* in this paper. In the state TR, several corrective inspections are tried in parallel with services. If the system is diagnosed as failure, the state moves to F, the service operation is stopped, and the recovery operation starts immediately. After completing the recovery from the system failure, the system becomes as good as new in G. Otherwise, it goes to the so-called non-failure state denoted by C_2. Here, two states can be taken; it may be switched to the gracefully service degradation in GD with probability q $(0 \leq q \leq 1)$, or the service operation is forced to stop and the corrective maintenance starts immediately.

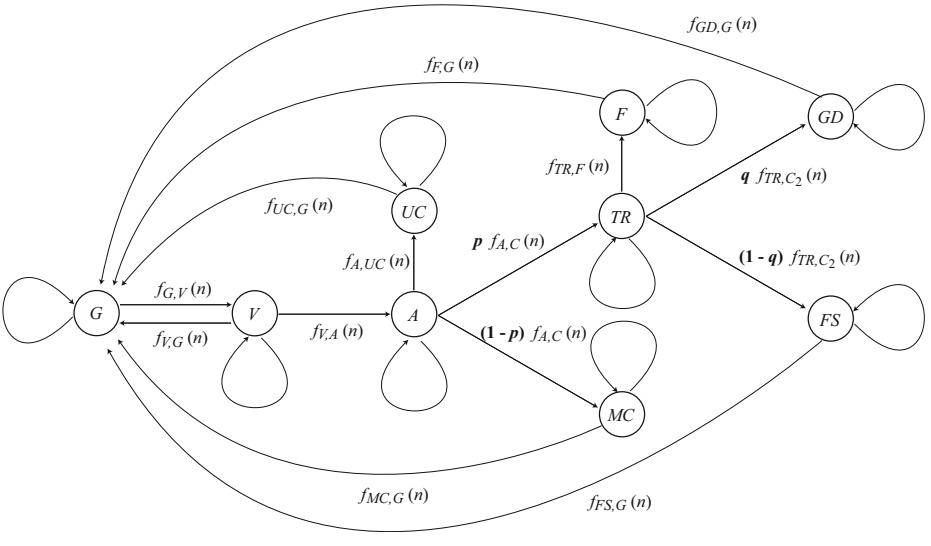

Fig. 2. Transition diagram of DTSMM

The main differences from Madan *et al.* [5], [6] are (i) an automatic intrusion-detection can be switched to a manual detection mode at any timing in A, although Madan *et al*. [5], [6] did not take account of switching of automatic detection mode, (ii) In two states C and C_2 instantaneous transitions are allowed in the present model, although Madan *et al*. [5], [6] assumed random transitions with time delay. We define the time interval from G to G as one cycle and suppose that the same cycle repeats again and again over an infinite time horizon. For respective states, let $F_{i,j}(n)$ $(i, j \in \{G, V, A, PM, UC, C, MC, TR, C_2, FS, GD, F\}$ denote the discrete transition probability distributions with p.m.f. $f_{i,j}(n)$ in the DTSMM, where $f_{i,j}(0) = 0$ and mean $\mu_{i,j}$ (> 0).

In Fig. 2, we give the trandition diagram of the DTSMM. It is assumed that the automatic detection function in SITAR is switched just after n_0 (≥ 0) time unit elapses in an active attack state A in the DTSMM. More specifically, let $F_{A,UC}(n)$ be the transition probability from A to UC which denotes the manual detection mode. When it is given by the step function, *i.e.*, $F_{A,UC}(n) = 1$ $(n \geq n_0)$ and $F_{A,UC}(n) = 0$ $(n < n_0)$, the switching time from an automatic detection mode to a manual detection model is given by the (integer-valued) constant time n_0. From the preliminary above, we formulate the steady-state system availability as a function of the switching time n_0.

3 Availability Analysis

3.1 EMC Approach

The embedded DTMC representation of the DTSMM is illustrated in Fig.3. Let p_k, h_k and π_k denote the steady-state probability of the DTSMM in Fig.2, the mean sojourn time and the steady-state probability of the embedded DTMC in Fig. 3, respectively, where $k \in \{G, V, A, DL, MC, TR, FS, GD, F\}$. From the definition, we can derive the the steady-state probability π_k of the DTSMM by

$$\pi_G = h_G/\phi, \tag{1}$$
$$\pi_V = h_V/\phi, \tag{2}$$
$$\pi_A = p_A h_A/\phi, \tag{3}$$
$$\pi_{DL} = p_A(1 - p_{MC} - p_{TR})h_{DL}/\phi, \tag{4}$$
$$\pi_{MC} = p_A p_{MC} h_{MC}/\phi, \tag{5}$$
$$\pi_{TR} = p_A p_{TR} h_{TR}/\phi, \tag{6}$$
$$\pi_{FS} = p_A p_{TR} p_{FS} h_{FS}/\phi, \tag{7}$$
$$\pi_{GD} = p_A p_{TR} p_{GD} h_{GD}/\phi, \tag{8}$$
$$\pi_F = p_A p_{TR}(1 - p_{FS} - p_{GD})h_F/\phi, \tag{9}$$

where

$$\phi = h_G + h_V + p_A\Big[h_A + (1 - p_{MC} - p_{TR})h_{DL} + p_{MC}h_{MC} + p_{TR}\Big\{h_{TR} + p_{FS}h_{FS} + p_{GD}h_{GD} + (1 - p_{FS} - p_{GD})h_F\Big\}\Big]. \tag{10}$$

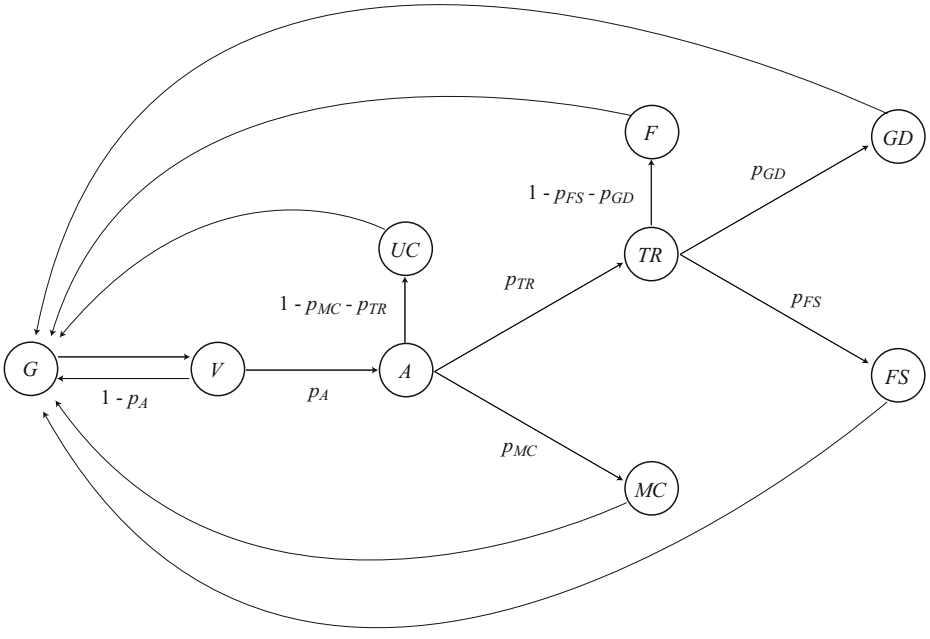

Fig. 3. EMC representation

3.2 Semi-markov Model

From the transition diagram of the DTSMM in Fig.3, we obtain

$$p_A = \sum_{x=0}^{\infty} \sum_{w=x}^{\infty} f_{V,G}(w) f_{V,A}(x), \tag{11}$$

$$p_{MC} = p_{MC}(n_0) = (1-p) F_{A,C}(n_0 - 1), \tag{12}$$

$$p_{TR} = p_{TR}(n_0) = p F_{A,C}(n_0 - 1), \tag{13}$$

$$p_{FS} = (1-q) \sum_{z=0}^{\infty} \sum_{y=z}^{\infty} f_{TR,F}(y) f_{TR,C_2}(z), \tag{14}$$

$$p_{GD} = q \sum_{z=0}^{\infty} \sum_{y=z}^{\infty} f_{TR,F}(y) f_{TR,C_2}(z) \tag{15}$$

and

$$h_G = \mu_{G,V}, \tag{16}$$

$$h_V = \sum_{x=0}^{\infty} \sum_{w=0}^{x-1} w f_{V,G}(w) f_{V,A}(x) + \sum_{x=0}^{\infty} \sum_{w=x}^{\infty} x f_{V,G}(w) f_{V,A}(x), \tag{17}$$

$$h_A = h_A(n_0) = \sum_{n=0}^{n_0-1} \overline{F}_{A,C}(n), \tag{18}$$

$$h_{DL} = \mu_{UC,G}, \tag{19}$$

$$h_{MC} = \mu_{MC,G}, \tag{20}$$

$$h_{TR} = \sum_{z=0}^{\infty}\sum_{y=0}^{z-1} y f_{TR,F}(y) f_{TR,C_2}(z) + \sum_{z=0}^{\infty}\sum_{y=z}^{\infty} z f_{TR,F}(y) f_{TR,C_2}(z), \tag{21}$$

$$h_{FS} = \mu_{FS,G}, \tag{22}$$

$$h_{GD} = \mu_{GD,G}, \tag{23}$$

$$h_F = \mu_{F,G}, \tag{24}$$

where $\overline{F}_{A,C}(n) = 1 - F_{A,C}(n)$. Then it is straightforward to get the steady-state system availability as a function of n_0 by

$$AV(n_0) = \pi_G + \pi_V + \pi_A + \pi_{MC} + \pi_{TR} + \pi_{GD} = U(n_0)/T(n_0), \tag{25}$$

where

$$U(n_0) = H_{G,V} + \sum_{x=0}^{\infty}\sum_{w=x}^{\infty} f_{V,G}(w) f_{V,A}(x) \Big\{ \sum_{n=0}^{n_0-1} \overline{F}_{A,C}(n) + \alpha F_{A,C}(n_0 - 1) \Big\}, \tag{26}$$

$$\begin{aligned} T(n_0) = H_{G,V} + \sum_{x=0}^{\infty}\sum_{w=x}^{\infty} f_{V,G}(w) f_{V,A}(x) \Big\{ & \sum_{n=0}^{n_0-1} \overline{F}_{A,C}(n) \\ & + \mu_{DL,G} \overline{F}_{A,C}(n_0 - 1) + \beta F_{A,C}(n_0 - 1) \Big\}, \end{aligned} \tag{27}$$

$$\overline{F}_{A,C}(n) = 1 - F_{A,C}(n-1) = \sum_{k=n}^{\infty} f_{A,C}(k), \tag{28}$$

$$h_{G,V} = \mu_{G,V} + \sum_{n=0}^{\infty} n f_{V,A}(n) \overline{F}_{V,G}(n) + \sum_{n=0}^{\infty} n f_{V,G}(n) \overline{F}_{V,A}(n), \tag{29}$$

$$\alpha = (1-p) h_{MC} + p(h_{TR} + p_{GD} h_{GD}), \tag{30}$$

$$\beta = \alpha + p\Big\{ p_{FS} h_{FS} + (1 - p_{FS} - p_{GD}) h_F \Big\}. \tag{31}$$

In the above expressions, α and β mean that the mean up time and the total mean time length from state C to G, respectively.

3.3 Optimal Switching Time

Taking the difference of $AV(n_0)$ with respect to n_0, we define

$$\begin{aligned} q(n_0) = & \Big\{ 1 + (\alpha - 1) r_{A,C}(n_0) \Big\} T(n_0) \\ & - U(n_0) \Big\{ 1 + (\beta - \mu_{DL,G} - 1) r_{A,C}(n_0) \Big\}, \end{aligned} \tag{32}$$

where $r_{A,C}(n_0) = f_{A,C}(n)/\overline{F}_{A,C}(n)$ is the discrete hazard rate. We make the following two parametric assumptions:

Table 1. Dependence of steady-state system availability on parameter r in discrete-time operation

	Case 1			Case 2		
r	n_0^*	$AV(n_0^*)$	Δ (%)	n_0^*	$AV(n_0^*)$	Δ (%)
1	∞	1	0	1	0.9322	0.0788
2	∞	1	0	8	0.9328	0.0162
3	∞	1	0	17	0.9338	0.0071
4	∞	1	0	25	0.9348	0.0043
5	∞	1	0	32	0.9358	0.0031

	Case 3			Case 4		
r	n_0^*	$AV(n_0^*)$	Δ (%)	n_0^*	$AV(n_0^*)$	Δ (%)
1	1	0.9322	10.5087	1	0.9322	3.5860
2	1	0.9322	10.1917	1	0.9322	3.4108
3	1	0.9322	9.8861	1	0.9322	3.2414
4	2	0.9324	9.6078	3	0.9326	3.1157
5	3	0.9327	9.3587	5	0.9330	3.0072

(A-1) $\alpha + \mu_{DL,G} < \beta$,
(A-2) $\alpha\mu_{DL,G} < h_{G,V}(\beta - \alpha - \mu_{DL,G})$.

From the definition it is evident that $\alpha < \beta$. The assumption **(A-1)** implies that the sum of mean up time after state C and the mean time overhead for switching to a manual detection mode is strictly smaller than the total mean time length. On the other hand, the assumption **(A-2)** seems to be somewhat technical but is needed to guarantee a unique optimal switching time. These both assumptions were numerically checked and could be validated in many parametric cases.

We characterize the optimal switching time from an automatic detection mode to a manual detection mode maximizing the steady-state system availability as follows:

Proposition: (1) Suppose that $F_{A,C}(n)$ is strictly IHR (Increasing Failure rate), *i.e.*, the hazard rate $r_{A,C}(n)$ is strictly increasing in n, under **(A-1)** and **(A-2)**. (i) If $q(0) > 0$ and $q(\infty) < 0$, then there exist (at least one, at most two) optimal switching time n_0^* ($0 < n_0^* < \infty$) satisfying the simultaneous inequalities $q(n_0^* - 1) > 0$ and $q(n_0^*) \leq 0$. The corresponding steady-state system availability $AV(n_0^*)$ must satisfy

$$K(n_0^* + 1) \leq AV(n_0^*) < K(n_0^*), \tag{33}$$

where

$$K(n) = \frac{1 + (\alpha - 1)r_{A,C}(n)}{1 + (\beta - \mu_{DL,G} - 1)r_{A,C}(n)}. \tag{34}$$

(ii) If $q(0) \leq 0$, then the optimal switching time is $n_0^* = 0$, *i.e.*, it is always optimal to detect in only a manual mode, and the corresponding maximum steady-state system availability is given by

$$AV(0) = \frac{h_{G,V}}{H_{G,V} + \mu_{DL,G} \sum_{x=0}^{\infty} \sum_{w=x}^{\infty} f_{V,G}(w) f_{V,A}(x)}. \tag{35}$$

Table 2. Dependence of steady-state system availability on parameter ξ in discrete-time operation

	Case 1			Case 2		
ξ	n_0^*	$AV(n_0^*)$	Δ (%)	n_0^*	$AV(n_0^*)$	Δ (%)
0.01	∞	1	0	∞	0.9692	0
0.05	∞	1	0	∞	0.9439	0
0.2	∞	1	0	17	0.9338	0.0071
0.5	∞	1	0	2	0.9323	0.1113

	Case 3			Case 4		
ξ	n_0^*	$AV(n_0^*)$	Δ (%)	n_0^*	$AV(n_0^*)$	Δ (%)
0.01	111	0.9470	2.1128	∞	0.9531	0
0.05	8	0.9335	7.2209	15	0.9346	1.9234
0.2	1	0.9322	9.8861	1	0.9322	3.2414
0.5	1	0.9322	10.5898	1	0.9322	3.6307

(iii) If $q(\infty) \geq 0$, then the optimal switching time is $n_0^* \to \infty$, *i.e.*, it is always optimal to detect in only an automatic mode, and the corresponding maximum steady-state system availability is given by

$$AV(\infty) = \frac{h_{G,V} + (\mu_{A,C} + \alpha)\sum_{x=0}^{\infty}\sum_{w=x}^{\infty} f_{V,G}(w) f_{V,A}(x)}{H_{G,V} + (\mu_{A,C} + \beta)\sum_{x=0}^{\infty}\sum_{w=x}^{\infty} f_{V,G}(w) f_{V,A}(x)}. \tag{36}$$

(2) Suppose that $F_{A,C}(n)$ is DHR (Decreasing hazard Rate), *i.e.*, the hazard rate $r_{A,C}(n)$ is decreasing in n, under **(A-1)** and **(A-2)**. If $AV(0) > AV(\infty)$, then $n_0^* = 0$, otherwise, $n_0^* \to \infty$.

Proof: Taking the difference of Eq.(32), we obtain

$$\begin{aligned} &q(n_0+1) - q(n_0) = \\ &\sum_{x=0}^{\infty}\sum_{w=x}^{\infty} f_{V,G}(w) f_{V,A}(x) \Big[\{T(n_0+1) - T(n_0)\} - \{U(n_0+1) - U(n_0)\} \\ &+ r_{A,C}(n_0+1)\Big\{(\alpha-1)T(n_0+1) - (\beta - \mu_{DL,G} - 1)U(n_0+1)\Big\} \\ &+ r_{A,C}(n_0)\Big\{(\alpha-1)T(n_0) - (\beta - \mu_{DL,G} - 1)U(n_0)\Big\}\Big]. \end{aligned} \tag{37}$$

If $F_{A,C}(n)$ is strictly IHR, the r.h.s. of Eq.(37) is strictly negative under **(A-1)** and **(A-2)**, and the function $q(n_0)$ is strictly decreasing in n_0. Since the steady-state system availability $AV(n_0)$ is a strictly quasi-concave in n_0 in the sense of discrete, if $q(0) > 0$ and $q(\infty) < 0$, then there exists at least one at most two optimal switching time n_0^* $(0 < n_0^* < \infty)$ so as to satisfy $q(n_0^* - 1) > 0$ and $q(n_0^*) \leq 0$ which lead to the inequalities in Eq.(33). If $q(0) \leq 0$ or $q(\infty) \geq 0$, then the function $AV(n_0)$ decreases or increases, and the resulting optimal switching time becomes $n_0^* = 0$ or $n_0^* \to \infty$. On the other hand, if $F_{A,C}(n)$ is DHR, the function $AV(n_0)$ is a quasi-convex function of n_0 in the sense of discrete, and the optimal switching time is given by $n_0^* = 0$ or $n_0^* \to \infty$.

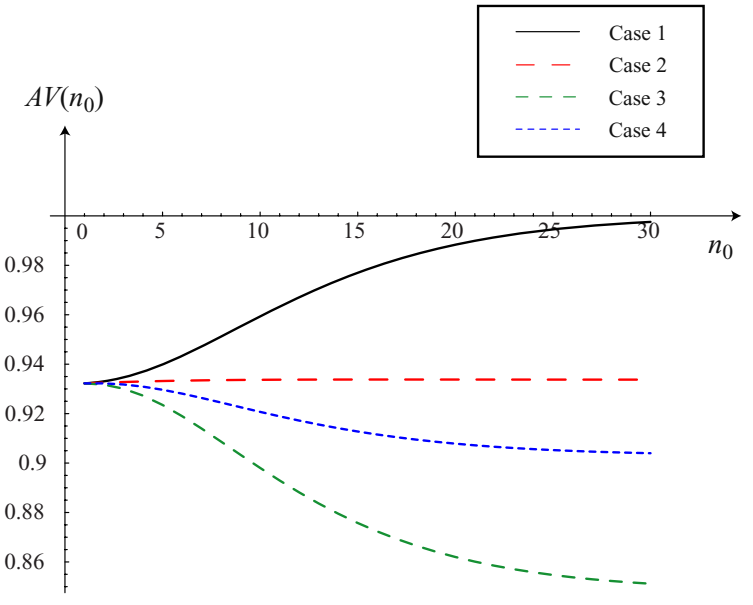

Fig. 4. Behavior of system availability $AV(n_0)$

4 Numerical Examples

In this section we derive the optimal switching time n_0^* numerically and quantify the steady-state system availability. Suppose the following parametric circumstance: $\mu_{G,V} = 72\text{C}\mu_{V,G} = 15\text{C}\ \mu_{V,A} = 24\text{C}\mu_{DL,G} = 15\text{C}\mu_{MC,G} = 12\text{C}\mu_{TR,F} = 6\text{C}\mu_{TR,C_2} = 8\text{C}\mu_{FS,G} = 30$, $\mu_{GD,G} = 40$ and $\mu_{F,G} = 48$. Especially we concern the following four cases:

(i) Case 1: $p = 0$, *i.e.*, the system state makes a transition from C to MC with probability one.

(ii) Case 2: $p = 0.5$ and $q = 0.5$.

(iii) Case 3: $p = 1$ and $q = 0$, *i.e.*, the service operation at C_2 is forced to stop with probability one.

(iv) Case 4: $p = 1$ and $q = 1$, *i.e.*, the graceful degradation can be observed with probability one.

Suppose that $f_{A,C}(n)$ is given by the negative binomial p.m.f.:

$$f_{A,C}(n) = \binom{n-1}{r-1} \xi^r (1-\xi)^{n-r}, \tag{38}$$

where $\xi \in (0,1)$ and $r = 1, 2, \cdots$ is the natural number. Figure 4 illustrates the behavior of the steady-state system availability with respect to the switching time n_0. From

this figure, it can be checked that each behavior of $AV(n_0)$ is rather different from each other among four cases. Table 1 presents the dependence of optimal switching time and its associated system availability for varying the parameter r under four different scenarios, where the increment Δ is calculated by $\{AV(n_0^*) - AV(\infty)\}\times 100/AV(n_0^*)$. By switching from an automatic mode to a manual mode at the best timing, it is seen that the steady-state system availability can be improved more than the case without switching to the manual mode. Especially, in Case 3, it is worth noting that the system availability could be improved up to $\Delta = 10.5\%$. Further, we execute the sensitivity analysis of optimal switching time for varying ξ in Table 2. It could be observed that the system availability monotonically decreased as ξ increased and that the increment of system availability was remarkable in Case 3 and Case 4. From these quantitative results it can be concluded that the control of the switching time would be useful to improve the system availability.

5 Conclusion

In this paper we have considered an availability models of an intrusion tolerant system by introducing a control parameter called the switching time from an automatic detection mode to a manual detection mode. We have derived the optimal time analytically so as to maximize the steady-state system availability. We have also investigated quantitative effects of the optimal control of switching timing in numerical examples. The lesson learned from the numerical examples was that the optimal switching could improve the system availability effectively. Hence, it has been shown that the combination between an intrusion tolerance architecture and a control of detection mode was quite effective in some cases. In the future work, we will examine an effect of the optimal switching policy on the mean time to security failure which is an alternative dependability/security measure of intrusion tolerant systems.

Acknowledgments

This research was partially supported by the Ministry of Education, Science, Sports and Culture, Grant-in-Aid for Scientific Research (C), Grant No. 21510167 (2009–2011) and the Research Program 2008 under the Center for Academic Development and Cooperation of the Hiroshima Shudo University, Japan.

References

1. Avizienis, A., Laprie, J.C., Randell, B., Landwehr, C.: Basic concepts and taxonomy of dependable and secure computing. IEEE Transactions on Dependable and Secure Computing 1(1), 11–33 (2004)
2. Deswarte, Y., Powell, D.: Internet security: an intrusion-torelance approach. Proceedings of the IEEE 94(2), 432–441 (2006)
3. Jonsson, E., Olovsson, T.: A quantitative model of the security intrusion process based on attacker behavior. IEEE Transactions on Software Engineering 23(4), 235–245 (1997)

4. Littlewood, B., Brocklehurst, S., Fenton, N., Mellor, P., Page, S., Wright, D., Doboson, J., McDermid, J., Gollmann, D.: Towards operational measures of computer security. Journal of Computer Security 2(2/3), 211–229 (1993)
5. Madan, B.B., Goseva-Popstojanova, K., Vaidyanathan, K., Trivedi, K.S.: Modeling and quantification of security attributes of software systems. In: Proceedings of 32nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2002), pp. 505–514. IEEE CS Press, Los Alamitos (2002)
6. Madan, B.B., Goseva-Popstojanova, K., Vaidyanathan, K., Trivedi, K.S.: A method for modeling and quantifying the security attributes of intrusion tolerant systems. Performance Evaluation 56(1/4), 167–186 (2004)
7. Ortalo, R., Deswarte, Y., Kaaniche, M.: Experimenting with quantitative evaluation tools for monitoring operational security. IEEE Transactions on Software Engineering 25(5), 633–650 (1999)
8. Uemura, T., Dohi, T.: Quantitative evaluation of intrusion tolerant systems subject to DoS attacks via semi-Markov cost models. In: Denko, M.K., Shih, C.-S., Li, K.-C., Tsao, S.-L., Zeng, Q.-A., Park, S.-H., Ko, Y.-B., Hung, S.-H., Park, J.-H. (eds.) EUC-WS 2007. LNCS, vol. 4809, pp. 31–42. Springer, Heidelberg (2007)
9. Uemura, T., Dohi, T.: Optimizing security measures in an intrusion tolerant database system. In: Nanya, T., Maruyama, F., Pataricza, A., Malek, M. (eds.) ISAS 2008. LNCS, vol. 5017, pp. 26–42. Springer, Heidelberg (2008)
10. Uemura, T., Dohi, T., Kaio, N.: Availability modeling of an intrusion tolerant system with preventive maintenance. In: Sheu, S.-H., Dohi, T. (eds.) Advanced Reliability Modeling III – Global Aspect of Reliability and Maintainability, pp. 655–662. McGraw Hill, New York (2008)
11. Wang, F., Gong, F., Sargor, C., Goseva-Popstojanova, K., Trivedi, K.S., Jou, F.: SITAR: A scalable intrusion-tolerant architecture for distributed services. In: Proceedings of 2nd Annual IEEE Systems, Man and Cybernetics, Information Assurance Workshop, West Point, NY (June 2001)
12. Wang, H., Liu, P.: Modeling and evaluating the survivability of an intrusion tolerant database system. In: Gollmann, D., Meier, J., Sabelfeld, A. (eds.) ESORICS 2006. LNCS, vol. 4189, pp. 207–224. Springer, Heidelberg (2006)